MassPoint PLLC
LEGAL AND STRATEGY ADVISORY

www.masspointpllc.com

-Positioning clients optimally in a globalized environment.

LEGAL AND POLICY UPDATE | MARCH 14, 2019

House Bill Aims to "Protect" Non-Classified Federally Funded Academic Research Deemed "Sensitive" to U.S. National Security by Restricting Foreign Student Participation, Other Measures

Protect Our Universities Act:

- Creates a "National Security Technology Task Force."
- Restricts certain foreign and dual national student participation.
- Prohibits use of items produced by Chinese, Russian, and other foreign firms.
- Specifically prohibits use of Huawei, ZTE, and Kaspersky equipment and software.
- Lays groundwork for potential licensing of "sensitive" research under or additional to ITAR and Export Controls regimes.
- Empowers federal agencies to enforce research restrictions, including by reducing and cancelling federal funding.
- Provides for Congressional oversight through reporting.

Related MassPoint Publications

- What Academia Should Know About the DOJ's China Initiative
- Infographic: U.S.-China Trade and Policy Issues
- US-China Risks to American Academia Are So Real They Are Insurable
- Fundamental Research Regulation, National Security, and Technological Competition
- Brain Drain: Emerging Technologies Export Controls Could Spur Tech Inversions
- BIS Rulemaking on Emerging Technologies Export Controls-Analysis
- Tech Wars: Restrictions on Foreign Access to U.S. Technology

On March 12, Congressman Jim Banks (R-IN) introduced in the House of Representatives the "**Protect Our Universities Act of 2019**," a bill "to create a task force within the Department of Education to address the threat of foreign government influence and threats to academic research integrity on college campuses, and for other purposes" (the "**POUA**" or "**Bill**").[1]

Measures to Counter Foreign "Threats" to Academic Research Integrity

Citing foreign "threats" to academic research integrity in American academia, the POUA seeks to restrict foreign participation in non-classified, federally funded academic research that is or could be deemed "sensitive" to U.S. national security. Toward this end, the POUA seeks to: (1) establish a multi-agency task force to identify "sensitive" research, (2) restrict certain foreign students and entities from involvement in such research, (3) facilitate foreign threat information sharing with and "instruction" to academic institutions, (4) empower federal funding agencies to enforce restrictions, and (5) institute Congressional oversight through reporting to multiple House committees.[2] Each of these elements of the Bill are discussed below.

POUA Reflects Concerns About Foreign Access to and Participation in U.S. Technology and Innovation Pipelines

The POUA draws on and reflects concerns in the federal government and elsewhere about threats posed by foreign countries and associated individuals and entities—particularly China and to a lesser extent Russia. The Bill's findings draw on White House and other Executive Branch reports on foreign threats, including "academic espionage" (discussed here and here). Viewed in the context of recently adopted and ongoing legislative, regulatory, and policy measures to restrict certain foreign access to and participation in U.S. technology and innovation networks—including through the Foreign Investment Risk Review and Modernization Act (**FIRRMA**), the Export Control Reform Act of 2018 (**ECRA**), and statutory exclusions of Huawei, ZTE, and other Chinese firms from federal procurement and private supply chains—the POUA is thematically harmonious with previous

restrictive measures and seeks to extend them explicitly to academic research, an important wellspring scientific and technological innovation in the United States.

The POUA follows a letter last year from 26 senators to the Education Secretary urging the "Secretary of Education to, among other actions, 'immediately request (and require) information from . . . [over 50] U.S. universities involved in [research partnerships with Huawei Technologies], especially those receiving any federal research funding . . . to gather information related to whether any such funding is involved in a Huawei partnership, and whether any research personnel (including Chinese nationals . . .) are involved in these efforts.'" The Education Secretary's response was, reportedly, "lackluster" and prompted the introduction of the POUA.

As discussed below, whether or not the POUA becomes law in its current or in another form, the Bill is instructive insofar as it reflects and builds on concerns about threats posed by foreign nations and associated individuals and entities, viewed as adversaries of the United States, particularly in the area of technological innovation and related "economic" and "academic" espionage and influence.[3] Accordingly, academic institutions and parties in the federally funded research pipeline—including technology and other companies—should take note of the POUA as it reflects sentiments that have and likely will continue to permeate the political and policy climate.

Elements of the POUA

I. Congressional Findings

- The POUA finds that, *inter alia*, "[a]dversaries of the United States take advantage of a largely vulnerable academic system . . . [including] federally funded research that takes place on the campuses of institutions of higher learning." Relying on White House-reported data, the POUA notes that that more than "300,000" Chinese nationals attend U.S. universities or are employed at national labs and other research and innovation institutions annually, and that "Chinese nationals now account for approximately one third of foreign university and college students in the United States and about 25 percent of graduate students specializing in" STEM.

- The POUA finds further that foreign students from "adversarial" nations are suspectable to "'undue pressure or incentives to "divulge technology to their home nation or to use sensitive information to negatively impact the United States." Quoting the June 2018 White House Report on China's Economic Aggression, the Bill finds that "Chinese nationals" in particular may pose threats to national and economic security because the "Chinese state may seek to manipulate or pressure even unwilling Chinse nationals into becoming nontraditional information collectors that serve Beijing's military and strategic ambitions.'"

  As indicated in a prior MassPoint update, this language is notable, as the underlying premise—that Chinese nationals (and corporate entities) are, by virtue of the structure of the Chinese state and the Chinese government's role in the economy, business, and technological development, susceptible to being "coopted" to engage in academic or economic espionage or unauthorized U.S.-to-China information and technology transfers—could lead to measures that broadly exclude or scrutinize Chinese nationals and entities based on nationality.[4] Quoting the FBI Director, the POUA finds that the threat posed by Chinese "non-traditional intelligence collectors 'are exploiting the very open [U.S.] research and development environment,'" and constitutes a "whole-of-society" threat from China that merits a 'whole-of-society' response by the United States.

- Relying on a highly influential 2018 Defense Innovation Unit (**DUIx**) report, the POUA states that "'[a]cademia is an opportune environment for learning about science and technology . . . [and] as a result, Chinese . . . students frequently master technologies that later become critical to key military systems, amounting over time to unintentional violations of U.S. export control laws.'"[5]

II. Scope: "Sensitive Research Projects," Requires Further Definition

- The Bill states that "technology and information that could be deemed sensitive to the national security interests of the United States should be given increased scrutiny to determine if access should be restricted." Consistent with that and other findings, the POUA seeks to restrict foreign access to and participation in projects that constitute a "Sensitive Research Project" which "means a research project at an institution of higher education that is funded by a qualified funding agency," and is not classified or that requires a security clearance as a condition of participation. As this short definition shows, "sensitive" to national security is not defined or described by illustration or otherwise and the Bill leaves it to a multi-agency task force to define the term. The open definitional issue—while not uncommon in legislation—in key ways mirrors the legislative approach to "emerging technologies" like Artificial Intelligence that, under ECRA, would be subject to export control if deemed "emerging technologies" that are "essential to national security" by the Department of Commerce, acting through an interagency process.

III. Department of Education Housed Inter-Agency Task Force; Sensitive Research Projects List

- The POUA would create within the Department of Education an inter-agency National Security Technology Task Force comprised of, in addition to the Department of Education and an intelligence community representative designated by the Director of National Intelligence (**DNI**), representatives from the Departments of Defense, Justice, and Energy (the "**Task Force**"), as well as others that may be designated. The Task Force must be established no later than one year from the date of the POUA's enactment, and a list of its members must be provided to Congress within ten days of its first meeting.

- Importantly, Task Force is required to, in consultation with the DNI, "actively maintain a list of sensitive research projects" and indicate, as to each project: (1) the relevant federal funding agency; (2) the openness of the project to student participation; and, (3) whether the project (i) "is related to an item listed on the Commerce Control List" (**CCL**) of export controlled items administered by the Department of Commerce in accordance with the Export Administration Regulations (**EAR**); (ii) "an item listed on the United States Munitions List" (**USML**) administered by the Department of State pursuant to the International Traffic in Arms Regulations (**ITAR**); or, (iii) "technology designated by the Secretary of Defense as having a technology readiness level of 1, 2, or 3."

- The Bill also requires the Task Force to, at least every six months, provide to affected academic institutions with "instruction" comprised of information about any relevant "threat posed by espionage, best practices identified by the Task Force [to combat foreign threats], and . . . any specific risks that the intelligence community, the qualified funding agency, or law enforcement entities determine appropriate to share with the institutions."

- The POUA requires the Task Force to report annually to multiple Congressional committees on the "threat of espionage at institutions of higher education" and "any action hat may be taken to reduce espionage carried out through student participation in sensitive research projects."[6]

  Notably, such reports must also include "an assessment of whether the current licensing regulations relating to" the ITAR and EAR "are sufficient to protect the security of the projects listed on the Sensitive Projects List." This language is important as, through legislatively mandated reporting, Congress not only conducts oversight but also gathers information to inform future legislative measures. Any reports or findings—whether provided pursuant to the POUA (if it becomes law) or any similar measures—could potentially inform academic research-specific export or other national security-based licensing or information/technology regimes, such as by expanding the scope of the EAR or ITAR, or adopting separate frameworks applicable specifically to federally funded research (and,

presumably, the fruits thereof). Any such developments—including any further hints of such potential measures—are worth carefully watching, not only by academia, but also by industry.

IV. Restrictions on Foreign Student Participation in Sensitive Research Projects

- **Foreign Student Restrictions, Designated Countries**. The POUA requires that all students participating in a Sensitive Research Project (**SRP**) provide "proof of citizenship" as a condition of participation and before participating. The onus of collecting proof of citizenship is on the "head" of an SRP at a relevant academic institution. Students with current or prior citizenship ties to four named countries, as well as other countries that may be "identified" by the "head" of a "qualified funding agency," are subject to stricter prerequisites to participation in SRPs. Specifically, students who are ***or have in the past been*** citizens or permanent residents of China, North Korea, Russia, and Iran (as well as countries designated in the future) are prohibited from participating in SRPs unless they first:

(1) Apply for and receive approval from the DNI to participate, "based on a background check and any other information" the DNI "determines to be appropriate," and

(2) *If the SRP "is related to an item or technology" listed on the CCL or USML, or is designated by the Defense Secretary as having a technology readiness level of 1, 2, or 3*, "the student [also] applies for and receives approval from the head of a qualified funding agency" to participate.

- **Problematic Citizenship-Based Restriction**. The Bill defines the term "citizen of a country" to include ***current and prior*** foreign country citizenship or permanent residency. The plain language of the Bill applies not only to individuals who are presently dual nationals of the United States and a designated country, but also current U.S. citizens who previously held citizenship or permanent residency in a designated country. Thus, for example, a U.S. citizen (with no other current foreign citizenship or residency) who was previously a citizen of Russia would be required to meet the applicable approval requirement(s) of the Bill, unlike other U.S. citizens who may have never held foreign citizenship or residency. Not only would this provision likely trigger discrimination issues, but institutions of higher education would also be in the undesirable (and arguably legally untenable) position of having to treat students differently, even where students otherwise are similarly situated vis-à-vis the academic institution. Or, such institutions may decide to forego federal funding for specific research projects. Presumably, should the POUA or any similar law advance in Congress, any foreign citizenship-based restrictions would likely be curtailed.

V. Prohibition on Federal Funding of Sensitive Research Utilizing Technologies "Developed" By Designated Entities Including Huawei, ZTE, and Kaspersky

- **Prohibited Entity List**. The POUA requires the DNI to develop and maintain a list of foreign government, corporate, non-profit, and other entities (and their affiliates and subsidiaries) that the DNI determines "pose a threat of espionage with respect to" SRMs. The DNI may add or remove entities from the list. However, the list must include the following entities and their subsidiaries and affiliates:

(1) Huawei (China),

(2) ZTE (China),

(3) Hytera Communications (China),

(4) Hikvision Digital Technology (China),

(5) Dahua Technology Company (China),[7]

(6) Kaspersky Lab, and

(7) "Any entity that is owned or controlled by, or otherwise has demonstrated financial ties to, the government of China, North Korea, Russia, Iran, or any other country identified by the head of a "qualified funding agency."

"As a condition of receipt of" federal funding, the head of an SRP must "provide assurance . . . that . . . any technology developed by an entity included on the list . . . shall not be utilized in carrying out" the SRP.

VI. Federal Funding Agencies' Enforcement Authority

The heads of federal funding agencies are empowered by the POUA to "take such steps as may be necessary to enforce" the foreign student and entity prohibitions of the Bill. Where a federal funding agency determines that the head of an SRP has "failed to meet" the POUA's relevant requirements, the agency head may "determine the appropriate enforcement action, including" (1) imposing a probationary period on the SRP or the head of the SRP for up to six months, (2) reducing or limiting funding until a violation is cured, (3) "permanently cancelling the funding for such project," or (4) "any other action" the agency head deems appropriate.

VII. Key Takeaways

The POUA may or may not progress in Congress, but its introduction is nevertheless notable for a number of reasons, including the following.

- First, the POUA underscores the fact that the "trade war" and, more pertinently, the tech war, between the United States and China has effects beyond commerce and military affairs. Academia, as in the case of the DOJ's China Initiative, is directly affected. Further, the POUA shows that, at least among some in government, current regulation of federally funded academic research is not beyond legislative or administrative interest and reach.
- Second, the POUA, like ECRA and the regulatory process underway to identify "emerging technologies" that are essential national security, would present difficulties in determining what constitutes research that is "sensitive" to national security—*e.g.*, does such research pertain only to that with clear military significance, encompass information that has "dual use" significance and application, or does sensitive research also include that which would contribute to the maintenance of the United States' technological edge relative to other countries?[8]
- Third, the effects of any changes to the regulation of participation in federally funded research would not be limited to academia. Commercial actors that directly and indirectly participate in such academic research or related commercialization are likely to be affected as well.

Universities, colleges, and research institutions should take note of the POUA and, more importantly, the legal, policy, and political sentiments and trends from which it stems. The POUA may not become a law with which academia will be required to contend (or comply with), but other laws or policies with similar objectives may soon materialize, if concerns persist about foreign (particularly Chinese) participation in and access to information and technology with national security or economic security significance. ■

Author Contact

To learn more about the matters discussed in this update or MassPoint's related services, please contact Hdeel Abdelhady at habdelhady@masspointpllc.com.

Explore Related MassPoint Publications by Topic

U.S.-CHINA LAW & POLICY • ACADEMIC ESPIONAGE • HIGHER ED LAW • TECH WAR • NATIONAL SECURITY LAW • TECHNOLOGY EXPORT CONTROLS

NOTES

[1] H.R. 1678, *available at* https://banks.house.gov/uploadedfiles/updated_huawei.pdf. The Bill was referred on March 12 to the House Committees on Education and Labor, Intelligence (Permanent Select), Armed Services, and, Science, Space, and Technology. The POUA to date has three co-sponsors: Representatives Trent Kelly (R-MS), Paul Cook (R-CA-8), and Don Bacon (R-NE). ("Huawei" in the file name might suggest that Huawei was of primary interest to the Bill's drafter(s)).

[2] These are the same House committees listed above, in note 1.

[3] For background on foreign "adversaries" and the various threats they have been deemed to pose to U.S. national security, "economic security," and technology and innovation, see the National Security Strategy of the United States, published by the White House in December 2017 ("**NSS**"). References in the POUA to "adversaries" is consistent with the NSS and other documents and statements that appear to have influenced or been influenced by the NSS.

[4] In Huawei's recently filed complaint challenging provisions of the National Defense Authorization Act that exclude Huawei (and ZTE and other Chinese entities from federal and, effectively, certain private supply chains) the company appears to argue, *inter alia*, that the NDAA wrongly treats Huawei as a state-controlled entity and, in doing so, infringes on the "separation of powers" by "legislatively adjudicating" Huawei's status vis-à-vis the Chinese state. The relevant NDAA provision is discussed in Hdeel Abdelhady, Tech Wars: Restrictions on Foreign Access to U.S. Technology, Law360, Oct. 18, 2018. Huawei's lawsuit is reminiscent of one filed previously by Russia's Kaspersky Labs, challenging a provision in an earlier NDAA, the National Defense authorization Act for Fiscal Year 2018, that prohibited federal agencies from using Kaspersky products and services. Kaspersky's case was dismissed and the dismissal was affirmed on appeal. *Kaspersky Lab, Inc. v. United States Dep't of Homeland Sec.*, 311 F. Supp. 3d 187 (D.D.C. 2018), *aff'd*, 909 F.3d 446 (D.C. Cir. 2018)

[5] The DUIx's January 2018 report, China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation, has been cited frequently in, among other places, Executive Branch reports, Congressional hearings, and draft legislation.

[6] The first report is due no later than one year after the law's enactment. As the same one-year outer deadline applies to the establishment of the Task Force, presumably deadlines would be modified if and as the Bill is modified.

[7] The Chinese companies listed are excluded from federal procurement and certain private procurement by the NDAA for FY 2019, as discussed in Hdeel Abdelhady, Tech Wars: Restrictions on Foreign Access to U.S. Technology, Law360, Oct. 18, 2018. Some senators have called for the imposition of Global Magnitsky Sanctions on Dahua, Hikvision, and Hytera for their provision of surveillance and other equipment to the Chinese government in connection with the Chinese government's abuses of Uighur and other Muslim minorities' human rights in China's Xinjiang province, as discussed in this MassPoint post on Legal and Reputation Risks in Technology Supply Chains.

[8] As discussed in MassPoint's update on the regulatory process for identifying "emerging technologies" essential to national security, ECRA states that the maintenance of the United States' comparative technological advantage is a "national security" interest.